In the claims:

Please amend the claims as follows.

1. (Amended) A method for protecting a network from a virus contained in an e-mail message as executable code, the method comprising:

(a) receiving the e-mail message in a gatekeeper server;

(b) converting the e-mail message from an executable format to a non-executable format by using one of a plurality of application-level conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message; and

(c) forwarding the non-executable format to the recipient of the e-mail message.

2. (Original) The method of claim 1, wherein the executable code is contained in a body of the e-mail message.

3. (Original) The method of claim 2, wherein the executable code comprises a hypertext link, and wherein step (b) comprises deactivating the hypertext link.

4. (Original) The method of claim 1, wherein the executable code is contained in an attachment in the e-mail message.

5. (Previously presented) The method of claim 4, wherein step (b) comprises:

(i) providing a plurality of sacrificial servers in communication with the gatekeeper server;

(ii) forwarding the attachment from the gatekeeper server to one of the plurality of sacrificial servers; and

(iii) converting the attachment to the non-executable format on said one of the plurality of

sacrificial servers by using said one of the plurality of conversion processes selected in accordance with the type of the e-mail message, the non-executable format retaining the appearance, human readability and semantic content of the e-mail message.

7. ~~6.~~ (Original) The method of claim 5, wherein step (b) further comprises (iii) examining the sacrificial server for virus activity.

8. ~~7.~~ (Original) The method of claim 7 ~~6~~, wherein step (b) further comprises (iv) rebooting the sacrificial server from a safe copy of an operating system obtained from a read-only device.

9. ~~8.~~ (Original) The method of claim 5, wherein communications between the gatekeeper server and the sacrificial server are authenticated using a challenge-and-response technique.

10. ~~9.~~ (Previously presented) The method of claim 4, wherein step (b) comprises:

B1

(i) maintaining a list of approved attachment file types and extensions;

(ii) determining whether the attachment is of a type or extension which is in the list of approved attachment file types and extensions; and

(iii) if the attachment is not of a type or extension which is in the list of approved attachment file types and extensions, informing the recipient that a message containing a non-approved attachment has been received.

11. ~~10.~~ (Original) The method of claim 1, wherein step (b) comprises:

(i) maintaining a list of approved executable code;

(ii) determining whether the executable code is in the list of approved executable code; and

(iii) deactivating the executable code if the executable code is not in the list of approved executable code.

12. ~~11.~~ (Original) The method of claim 11 ~~10~~, wherein:

B

the list of approved executable code includes information for determining whether the approved executable code has been altered; and

step (b) further comprises:

(iv) determining whether the executable code has been altered; and

(v) deactivating the executable code if the executable code has been altered.

18. 12
~~12.~~ (Original) The method of claim ~~11~~, wherein step (b)(iv) is performed through an algorithmic technique.

14. 13
~~13.~~ (Original) The method of claim ~~12~~, wherein the algorithmic technique is a check-summing technique.

15. 13
~~14.~~ (Original) The method of claim ~~12~~, wherein the algorithmic technique is a hashing technique.

B1

16.
~~15.~~ (Original) The method of claim 1, wherein step (b) comprises:

(i) forming a first copy and a second copy of at least a portion of the e-mail message containing the executable code;

(ii) executing the executable code in the first copy but not the second copy; and

(iii) after the executable code in the first copy has been executed, comparing the first copy to the second copy to determine an effect of the executable code.

12

17.
~~16.~~ (Amended) A system for protecting a network from a virus contained in an e-mail message as executable code, the system comprising:

B

a workstation computer on the network used by a recipient of the e-mail message;

a gatekeeper server, in communication with the workstation computer over the network, for receiving the e-mail message; and

a computer on the network for converting the e-mail message from an executable format to a non-executable format by using one of a plurality of application-level conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and forwarding the converted e-mail message to the workstation computer.

~~17.~~ 18. (Original) The system of claim ~~16~~ 17, wherein the executable code is contained in a body of the e-mail message.

~~18.~~ 19. (Original) The system of claim ~~17~~ 18, wherein the executable code comprises a hypertext link, and wherein the computer for converting deactivates the hypertext link.

~~19.~~ 20. (Original) The system of claim ~~16~~ 17, wherein the executable code is contained in an attachment in the e-mail message.

~~20.~~ 21. (Previously presented) The system of claim ~~16~~ 17, wherein the computer for converting is one of a plurality of sacrificial servers which are in communication with the gatekeeper server.

~~21.~~ 22. (Previously presented) The system of claim ~~20~~ 21, wherein the plurality of sacrificial servers are examined for virus activity.

~~22.~~ 23. (Previously presented) The system of claim ~~21~~ 23, wherein the network further comprises a read-only device, and wherein the sacrificial servers are rebooted from a safe copy of an operating system obtained from the read-only device.

~~23.~~ 24. (Previously presented) The system of claim ~~20~~ 21, wherein communications between the

gatekeeper server and the sacrificial servers are authenticated using a challenge-and-response technique.

26 17
~~24.~~ (Previously presented) The system of claim ~~16,~~ wherein the network maintains a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, informs the recipient that a message containing a non-approved attachment has been received.

27 17
~~25.~~ (Original) The system of claim ~~16,~~ wherein the network maintains a list of approved executable code, determines whether the executable code is in the list of approved executable code, and deactivates the executable code if the executable code is not in the list of approved executable code.

B1

28 27
~~26.~~ (Original) The system of claim ~~25,~~ wherein:

the list of approved executable code includes information for determining whether the approved executable code has been altered;

the network determines whether the executable code has been altered; and

the executable code is deactivated if the executable code has been altered.

29 28
~~27.~~ (Original) The system of claim ~~26,~~ wherein the system determines whether the executable code has been altered through an algorithmic technique.

30 29
~~28.~~ (Original) The system of claim ~~27,~~ wherein the algorithmic technique is a check-summing technique.

31 29
~~29.~~ (Original) The system of claim ~~27,~~ wherein the algorithmic technique is a hashing

B

technique.

30. (Original) The system of claim 16, wherein the computer for converting converts the executable code by:

(i) forming a first copy and a second copy of at least a portion of the e-mail message containing the executable code;

(ii) executing the executable code in the first copy but not the second copy; and

(iii) after the executable code in the first copy has been executed, comparing the first copy to the second copy to determine an effect of the executable code.

31. (Amended) A sacrificial server for use on a network, the sacrificial server comprising:

communication means for receiving an e-mail attachment from the network; and

processing means for converting the e-mail attachment from an executable format to a non-executable format by using one of a plurality of application-level conversion processes selected in accordance with a type of the e-mail message, the non-executable format retaining an appearance, human readability and semantic content of the e-mail message and for returning the e-mail attachment to the network.

32. (Original) The sacrificial server of claim 31, wherein the sacrificial server is examined for virus activity.

33. (Original) The sacrificial server of claim 32, wherein the sacrificial server further comprises a read-only device and is rebooted from a safe copy of an operating system obtained

from the read-only device.

34. (Original) The sacrificial server of claim 31, wherein communications between the network and the sacrificial server are authenticated using a challenge-and-response technique.

35. (Previously presented) The sacrificial server of claim 31, wherein the sacrificial server stores a list of approved attachment file types and extensions, determines whether the attachment is of a file type or extension which is in the list of approved attachment file types and extensions, and, if the attachment is not of a file type or extension which is in the list of approved attachment file types and extensions, and informs the network that a message containing a non-approved attachment has been received.

36. (Original) The sacrificial server of claim 31, wherein the sacrificial server maintains a list of approved executable code, determines whether the attachment contains executable code and whether the executable code is in the list of approved executable code, and deactivates the executable code if the executable code is not in the list of approved executable code.

37. (Original) The sacrificial server of claim 36, wherein:

the list of approved executable code includes information for determining whether the approved executable code has been altered;

if the executable code is in the list of approved executable code, the sacrificial server determines whether the executable code has been altered; and

the executable code is deactivated if the executable code has been altered.

38. (Original) The sacrificial server of claim 32, wherein the sacrificial server determines whether the executable code has been altered through the use of an algorithmic technique.

39. (Original) The sacrificial server of claim 38, wherein the algorithmic technique is a

check-summing technique.

39. 36
~~40~~. (Original) The sacrificial server of claim ~~38~~, wherein the algorithmic technique is a hashing technique.

34. 33
~~41~~. (Original) The sacrificial server of claim ~~31~~, wherein the processing means converts the executable code by:

(i) forming a first copy and a second copy of at least a portion of the e-mail message containing the executable code;

(ii) executing the executable code in the first copy but not the second copy; and

31

(iii) after the executable code in the first copy has been executed, comparing the first copy to the second copy to determine an effect of the executable code.

6.
~~42~~. (Previously presented) The method of claim 5, wherein the plurality of sacrificial servers are separate from the gatekeeper server.

22. 21
~~43~~. (Previously presented) The system of claim ~~20~~, wherein the plurality of sacrificial servers are separate from the gatekeeper server.